PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-229451
(43)Date of publication of application : 14.08.2002

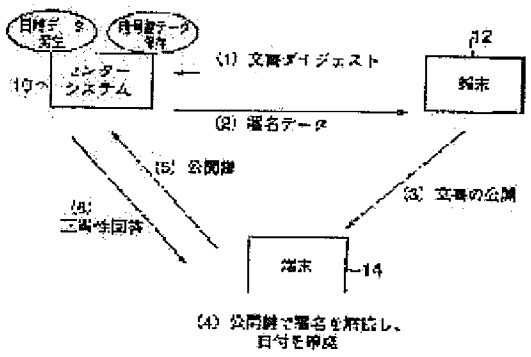
(51)Int.Cl. G09C 1/00
G06F 12/14
G06F 17/21
H04L 9/32

(21)Application number : 2001-027130
(22)Date of filing : 02.02.2001

(71)Applicant : CASIO COMPUT CO LTD
(72)Inventor : IIZUKA NORIO

(54) SYSTEM, METHOD, AND PROGRAM FOR GUARANTEEING DATE AND HOUR OF CREATION OF DATA

(57)Abstract:
PROBLEM TO BE SOLVED: To guarantee the date and hour of creation of data.
SOLUTION: When a center system 10 receives the guarantee request of the date and hour of the creation of a document, and a document digest subject to the guarantee from a terminal 12 (1), the center system 10 creates date and hour data, integrates them in a form indivisible from the document digest, creates signature data in which the date and hour data are encrypted on the basis of secret key data by a public key cryptosystem, and transmits them to the terminal 12 (2). When the terminal 12 publishes the document to a terminal 14, the terminal 12 attaches the signature data and public key data to document data and transmits them. When the center system 10 receives the public key data together with the guarantee request of the validity from the terminal 14 (5), the center system 10 discriminates whether or not the public key data is valid data corresponding to the secret key data used when the creating signature data from the document digest received from the terminal 12, and transmits the discrimination result to the terminal 14 which is the sender of the public key data (6).



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－229451
（P2002－229451A）
(43)公開日　平成14年８月14日(2002.8.14)

(51)Int.Cl.⁷		識別記号	Ｆｉ		テーマコード（参考）
Ｇ０９Ｃ	1/00	６４０	Ｇ０９Ｃ	1/00	６４０Ｚ　５Ｂ００９
					６４０Ｂ　５Ｂ０１７
Ｇ０６Ｆ	12/14	３１０	Ｇ０６Ｆ	12/14	３１０Ｚ　５Ｊ１０４
		３２０			３２０Ａ
	17/21	５９０		17/21	５９０Ｊ

審査請求　未請求　請求項の数15　ＯＬ　（全 16 頁）　最終頁に続く

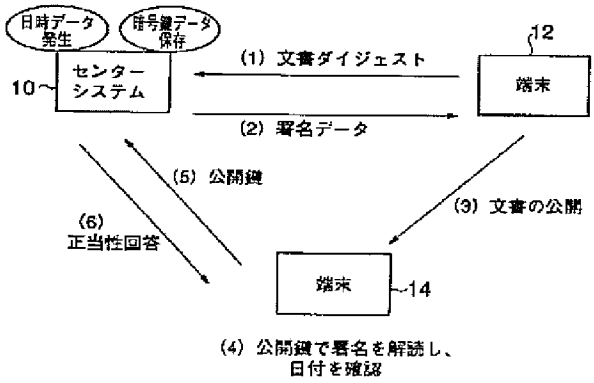
(21)出願番号　特願2001－27130(P2001－27130)
(22)出願日　平成13年２月２日(2001.2.2)

(71)出願人　000001443
カシオ計算機株式会社
東京都渋谷区本町１丁目６番２号
(72)発明者　飯塚　宣男
東京都羽村市栄町３丁目２番１号　カシオ計算機株式会社羽村技術センター内
(74)代理人　100058479
弁理士　鈴江　武彦　（外５名）

Ｆターム(参考)　5B009 TB13 VA03
5B017 AA08 BA07
5J104 AA09 LA03 LA05 LA06 MA02
NA02 PA07

(54)【発明の名称】　データ作成日時保証システム、データ作成日時保証方法、及びデータ作成日時保証プログラム

(57)【要約】
【課題】データの作成日時を保証できるようにする。
【解決手段】センターシステム１０は、端末１２より文書の作成日時の保証依頼と保証対象とする文書ダイジェストを受信すると（１）、日時データを作成して文書ダイジェストと不可分な形で統合し、これを公開鍵暗号方式による秘密鍵データをもとに暗号化した署名データを生成して端末１２送信する（２）。端末１２は、端末１４に対して文書を公開する場合には、文書データに署名データと公開鍵データとを添付して送信する。センターシステム１０は、端末１４から公開鍵データと共に正当性の保証依頼を受信すると（５）、端末１２から受信した文書ダイジェストから署名データを生成する際に用いた秘密鍵データに対応する正当なものであるかを判別し、その判別結果を公開鍵データの送信元である端末１４に送信する（６）。



1

【特許請求の範囲】

【請求項１】　端末において作成されたデータの作成日時を保証するデータ作成日時保証システムであって、
端末よりデータ作成日時の保証を受けようとするデータを受信するデータ受信手段と、
日時データを作成する日時データ作成手段と、
前記データ受信手段によって受信したデータと前記日時データ作成手段によって作成した日時データとを統合し、公開鍵暗号方式による秘密鍵データをもとに暗号化した署名データを生成する署名データ生成手段と、
前記署名データ生成手段によって生成された署名データを前記データ受信手段によって受信したデータの送信元に送信するデータ送信手段とを具備したことを特徴とするデータ作成日時保証システム。

【請求項２】　公開鍵暗号方式による公開鍵データと共に、この公開鍵データに関する正当性の保証依頼を受信する公開鍵データ保証依頼受信手段と、
前記公開鍵データ保証依頼受信手段によって受信した公開鍵データが、前記署名データ生成手段によって署名データを生成する際に用いた秘密鍵データに対応する正当なものであるかを判別する正当性判別手段と、
前記正当性判別手段による判別結果を、前記公開鍵データ保証依頼受信手段によって受信した公開鍵データの送信元に送信する判別結果送信手段とを具備したことを特徴とする請求項１記載のデータ作成日時保証システム。

【請求項３】　端末において作成されたデータの作成日時を保証するデータ作成日時保証システムであって、
端末よりデータ作成日時の保証を受けようとするデータを受信するデータ受信手段と、
日時データを作成する日時データ作成手段と、
前記データ受信手段によって受信したデータと前記日時データ作成手段によって作成した日時データとを統合し、公開鍵暗号方式による秘密鍵データをもとに暗号化した署名データを生成する署名データ生成手段と、
前記署名データ生成手段によって生成された署名データを格納する署名データ格納手段と、
前記署名データ格納手段によって格納された署名データを特定するためのリンク情報を前記データ受信手段によって受信したデータの送信元に送信するリンク情報送信手段とを具備したことを特徴とするデータ作成日時保証システム。

【請求項４】　前記署名データ格納手段によって格納された署名データを特定するためのリンク情報と前記署名データ生成手段による署名データの作成対象となったとしているデータと共に、このデータに関する正当性の保証依頼を受信するデータ保証依頼受信手段と、
前記データ保証依頼受信手段によって受信したデータが前記署名データ生成手段による署名データの生成の対象となった正当なものであるかを、前記データ保証依頼受信手段により受信した前記リンク情報が示す前記署名データ格納手段に格納された署名データをもとに判別する正当性判別手段と、
前記正当性判別手段による判別結果を、前記データ保証依頼受信手段によって受信したデータの送信元に送信する判別結果送信手段とを具備したことを特徴とする請求項３記載のデータ作成日時保証システム。

2

【請求項５】　端末において作成されたデータの作成日時を保証するデータ作成日時保証システムであって、
端末より日時データの要求を受信する要求受信手段と、
日時データを作成する日時データ作成手段と、
前記要求受信手段により受信した要求に応じて、前記日時データ作成手段によって作成された日時データを前記要求受信手段によって受信した要求の送信元に送信する日時データ送信手段とを具備したことを特徴とするデータ作成日時保証システム。

【請求項６】　公開鍵暗号方式による公開鍵データと共に、この公開鍵データに関する正当性の保証依頼を受信する公開鍵データ保証依頼受信手段と、
前記公開鍵データ保証依頼受信手段によって受信した公開鍵データが、端末において作成されたデータを暗号化する際に用いられる書き換え不能な記録媒体に記録された公開鍵暗号方式による秘密鍵データに対応する正当なものであるかを判別する正当性判別手段と、
前記正当性判別手段による判別結果を、前記公開鍵データ保証依頼受信手段によって受信した公開鍵データの送信元に送信する判別結果送信手段とを具備したことを特徴とする請求項５記載のデータ作成日時保証システム。

【請求項７】　データを作成する端末において、
作成したデータの作成日時の保証要求を入力する要求入力手段と、
前記要求入力手段によって保証要求が入力された場合に、日時データの要求を所定のシステムに対して送信する要求送信手段と、
前記要求送信手段による要求に対する前記システムからの日時データを受信する日時データ受信手段と、
暗号化プログラムと公開鍵暗号方式による秘密鍵データとが記録された記録内容を書き換え不能な記録媒体を用い、作成したデータと前記日時データ受信手段によって受信した日時データとを統合し、前記記録媒体に記録された秘密鍵データをもとに前記暗号化プログラムに従って暗号化した署名データを生成する署名データ生成手段とを具備したことを特徴とする端末。

【請求項８】　再現性のない事象をもとにした付加データを作成する付加データ作成手段と、
前記付加データ作成手段によって作成された付加データを前記日時データ作成手段によって作成された日時データと対応づけて格納する付加日時データ格納手段とを具備し、
前記日時データ送信手段は、前記日時データと共に前記付加データ作成手段によって作成された付加データを送

信することを特徴とする請求項５記載のデータ作成日時保証システム。

【請求項９】　日時データと付加データと共に、これらのデータに関する正当性の保証依頼を受信するデータ保証依頼受信手段と、

前記データ保証依頼受信手段によって受信した日時データと付加データとが正当なものであるかを、前記付加日時データ格納手段に格納された日時データと付加データとをもとに判別する付加日時データ正当性判別手段と、

前記付加日時判別データ正当性判別手段による判別結果を、前記データ保証依頼受信手段によって受信したデータの送信元に送信する判別結果送信手段とを具備したことを特徴とする請求項８記載のデータ作成日時保証システム。

【請求項１０】　端末において作成されたデータの作成日時を保証するデータ作成日時保証方法であって、

端末よりデータ作成日時の保証を受けようとするデータを受信するデータ受信ステップと、

日時データを作成する日時データ作成ステップと、

前記データ受信ステップによって受信したデータと前記日時データ作成ステップによって作成した日時データとを統合し、公開鍵暗号方式による秘密鍵データをもとに暗号化した署名データを生成する署名データ生成ステップと、

前記署名データ生成ステップによって生成された署名データを前記データ受信ステップによって受信したデータの送信元に送信するデータ送信ステップと、

公開鍵暗号方式による公開鍵データと共に、この公開鍵データに関する正当性の保証依頼を受信する公開鍵データ保証依頼受信ステップと、

前記公開鍵データ保証依頼受信ステップによって受信した公開鍵データが、前記署名データ生成ステップによって署名データを生成する際に用いた秘密鍵データに対応する正当なものであるかを判別する正当性判別ステップと、

前記正当性判別ステップによる判別結果を、前記公開鍵データ保証依頼受信ステップによって受信した公開鍵データの送信元に送信する判別結果送信ステップとを有することを特徴とするデータ作成日時保証方法。

【請求項１１】　端末において作成されたデータの作成日時を保証するためにコンピュータを、

端末よりデータ作成日時の保証を受けようとするデータを受信するデータ受信手段と、

日時データを作成する日時データ作成手段と、

前記データ受信手段によって受信したデータと前記日時データ作成手段によって作成した日時データとを統合し、公開鍵暗号方式による秘密鍵データをもとに暗号化した署名データを生成する署名データ生成手段と、

前記署名データ生成手段によって生成された署名データを前記データ受信手段によって受信したデータの送信元に送信するデータ送信手段と、

公開鍵暗号方式による公開鍵データと共に、この公開鍵データに関する正当性の保証依頼を受信する公開鍵データ保証依頼受信手段と、

前記公開鍵データ保証依頼受信手段によって受信した公開鍵データが、前記署名データ生成手段によって署名データを生成する際に用いた秘密鍵データに対応する正当なものであるかを判別する正当性判別手段と、

前記正当性判別手段による判別結果を、前記公開鍵データ保証依頼受信手段によって受信した公開鍵データの送信元に送信する判別結果送信手段とに機能させるためのデータ作成日時保証プログラム。

【請求項１２】　端末において作成されたデータの作成日時を保証するデータ作成日時保証方法であって、

端末よりデータ作成日時の保証を受けようとするデータを受信するデータ受信ステップと、

日時データを作成する日時データ作成ステップと、

前記データ受信ステップによって受信したデータと前記日時データ作成ステップによって作成した日時データとを統合し、公開鍵暗号方式による秘密鍵データをもとに暗号化した署名データを生成する署名データ生成ステップと、

前記署名データ生成ステップによって生成された署名データを格納する署名データ格納ステップと、

前記署名データ格納ステップによって格納された署名データを特定するためのリンク情報を前記データ受信ステップによって受信したデータの送信元に送信するリンク情報送信ステップと、

前記署名データ格納ステップによって格納された署名データを特定するためのリンク情報と前記署名データ生成ステップによる署名データの作成対象となったとしているデータと共に、このデータに関する正当性の保証依頼を受信するデータ保証依頼受信ステップと、

前記データ保証依頼受信ステップによって受信したデータが前記署名データ生成ステップによる署名データの生成の対象となった正当なものであるかを、前記データ保証依頼受信ステップにより受信した前記リンク情報が示す前記署名データ格納ステップに格納された署名データをもとに判別する正当性判別ステップと、

前記正当性判別ステップによる判別結果を、前記データ保証依頼受信ステップによって受信したデータの送信元に送信する判別結果送信ステップとを有することを特徴とするデータ作成日時保証方法。

【請求項１３】　端末において作成されたデータの作成日時を保証するためにコンピュータを、

端末よりデータ作成日時の保証を受けようとするデータを受信するデータ受信手段と、

日時データを作成する日時データ作成手段と、

前記データ受信手段によって受信したデータと前記日時データ作成手段によって作成した日時データとを統合

し、公開鍵暗号方式による秘密鍵データをもとに暗号化した署名データを生成する署名データ生成手段と、
前記署名データ生成手段によって生成された署名データを格納する署名データ格納手段と、
前記署名データ格納手段によって格納された署名データを特定するためのリンク情報を前記データ受信手段によって受信したデータの送信元に送信するリンク情報送信手段と、
前記署名データ格納手段によって格納された署名データを特定するためのリンク情報と前記署名データ生成手段による署名データの作成対象となったとしているデータと共に、このデータに関する正当性の保証依頼を受信するデータ保証依頼受信手段と、
前記データ保証依頼受信手段によって受信したデータが前記署名データ生成手段による署名データの生成の対象となった正当なものであるかを、前記データ保証依頼受信手段により受信した前記リンク情報が示す前記署名データ格納手段に格納された署名データをもとに判別する正当性判別手段と、
前記正当性判別手段による判別結果を、前記データ保証依頼受信手段によって受信したデータの送信元に送信する判別結果送信手段とに機能させるためのデータ作成日時保証プログラム。
【請求項１４】　端末において作成されたデータの作成日時を保証するデータ作成日時保証方法であって、
端末より日時データの要求を受信する要求受信ステップと、
日時データを作成する日時データ作成ステップと、
前記要求受信ステップにより受信した要求に応じて、前記日時データ作成ステップによって作成された日時データを前記要求受信ステップによって受信した要求の送信元に送信する日時データ送信ステップと、
公開鍵暗号方式による公開鍵データと共に、この公開鍵データに関する正当性の保証依頼を受信する公開鍵データ保証依頼受信ステップと、
前記公開鍵データ保証依頼受信ステップによって受信した公開鍵データが、端末において作成されたデータを暗号化する際に用いられる書き換え不能な記録媒体に記録された公開鍵暗号方式による秘密鍵データに対応する正当なものであるかを判別する正当性判別ステップと、
前記正当性判別ステップによる判別結果を、前記公開鍵データ保証依頼受信ステップによって受信した公開鍵データの送信元に送信する判別結果送信ステップとを有することを特徴とするデータ作成日時保証方法。
【請求項１５】　端末において作成されたデータの作成日時を保証するためにコンピュータを、
端末より日時データの要求を受信する要求受信手段と、
日時データを作成する日時データ作成手段と、
前記要求受信手段により受信した要求に応じて、前記日時データ作成手段によって作成された日時データを前記

要求受信手段によって受信した要求の送信元に送信する日時データ送信手段と、
公開鍵暗号方式による公開鍵データと共に、この公開鍵データに関する正当性の保証依頼を受信する公開鍵データ保証依頼受信手段と、
前記公開鍵データ保証依頼受信手段によって受信した公開鍵データが、端末において作成されたデータを暗号化する際に用いられる書き換え不能な記録媒体に記録された公開鍵暗号方式による秘密鍵データに対応する正当なものであるかを判別する正当性判別手段と、
前記正当性判別手段による判別結果を、前記公開鍵データ保証依頼受信手段によって受信した公開鍵データの送信元に送信する判別結果送信手段とに機能させるためのデータ作成日時保証プログラム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、端末において作成されたデータの日時を保証するデータ作成日時保証システム、データ作成日時保証方法、及びデータ作成日時保証プログラムに関する。
【０００２】
【従来の技術】近年、インターネットなどのネットワークの発達に伴い、ネットワークを介して様々なデータがコンピュータ間で送受信されている。重要なデータについは、データの正当性を証明するためのデジタル署名の技術が用いられており、生成されたデータの改ざん防止が図られている。
【０００３】デジタル署名は、データの送信者は、送信対象とするデータをもとにして公開鍵暗号方式における秘密鍵（かぎ）を用いて署名データを作成し、この署名データを送信対象とするデータに付けて送信する。受信者は、公開鍵を使って署名データを復号し、この復号化された署名データと受信したデータとをもとにして、署名データが正しい送信者が署名したものであり、データが改ざんされていないことを確認できる。
【０００４】また、公開鍵が正当であることを保証するために認証局という機関が設けられている。認証局は、公開鍵暗号方式に基づくデジタル署名を利用するときの公開鍵が正当であることを保証する証明書を発行する。受信者は、発信者が配布した公開鍵が認証局からの証明書付きであれば、公開鍵についても正当であることを確認することができる。
【０００５】
【発明が解決しようとする課題】しかしながら、従来のデジタル署名の技術は、データの作成者とデータの正当性を保証するものであって、データの作成日時を保証することができなかった。例えば特許出願しようとする開発技術に関して文書を作成した場合、文書作成時には非公開であるが、何れ公開する際に作成日時を保証できるようにしておきたいという要求がある。しかし、従来の

デジタル署名の技術では文書の内容が改ざんされていないという正当性を保証できても、文書の作成日時については保証することができなかった。

【０００６】通常、パーソナルコンピュータなどにおいてデータを作成した場合には、そのデータのファイルについてデータ更新日時を表すタイムスタンプが記憶されるが、コンピュータに搭載された時計が正確ではないことがあり、またファイルスタンプに対する変更が容易にできるために、精度と信頼性について満足できるものではなかった。

【０００７】本発明は、前記のような問題に鑑みなされたもので、データの作成日時を保証することができるデータ作成日時保証システム、データ作成日時保証方法、及びデータ作成日時保証プログラムを提供することを目的とする。

【０００８】

【課題を解決するための手段】本発明は、端末において作成されたデータの作成日時を保証するデータ作成日時保証システムであって、端末よりデータ作成日時の保証を受けようとするデータを受信するデータ受信手段と、日時データを作成する日時データ作成手段と、前記データ受信手段によって受信したデータと前記日時データ作成手段によって作成した日時データとを統合し、公開鍵暗号方式による秘密鍵データをもとに暗号化した署名データを生成する署名データ生成手段と、前記署名データ生成手段によって生成された署名データを前記データ受信手段によって受信したデータの送信元に送信するデータ送信手段とを具備する。

【０００９】また、公開鍵暗号方式による公開鍵データと共に、この公開鍵データに関する正当性の保証依頼を受信する公開鍵データ保証依頼受信手段と、前記公開鍵データ保証依頼受信手段によって受信した公開鍵データが、前記署名データ生成手段によって署名データを生成する際に用いた秘密鍵データに対応する正当なものであるかを判別する正当性判別手段と、前記正当性判別手段による判別結果を、前記公開鍵データ保証依頼受信手段によって受信した公開鍵データの送信元に送信する判別結果送信手段とを具備したことを特徴とする。

【００１０】また本発明は、端末において作成されたデータの作成日時を保証するデータ作成日時保証システムであって、端末よりデータ作成日時の保証を受けようとするデータを受信するデータ受信手段と、日時データを作成する日時データ作成手段と、前記データ受信手段によって受信したデータと前記日時データ作成手段によって作成した日時データとを統合し、公開鍵暗号方式による秘密鍵データをもとに暗号化した署名データを生成する署名データ生成手段と、前記署名データ生成手段によって生成された署名データを格納する署名データ格納手段と、前記署名データ格納手段によって格納された署名データを特定するためのリンク情報を前記データ受信手

段によって受信したデータの送信元に送信するリンク情報送信手段とを具備したことを特徴とする。

【００１１】また、前記署名データ格納手段によって格納された署名データを特定するためのリンク情報と前記署名データ生成手段による署名データの作成対象となったとしているデータと共に、このデータに関する正当性の保証依頼を受信するデータ保証依頼受信手段と、前記データ保証依頼受信手段によって受信したデータが前記署名データ生成手段による署名データの生成の対象となった正当なものであるかを、前記データ保証依頼受信手段により受信した前記リンク情報が示す前記署名データ格納手段に格納された署名データをもとに判別する正当性判別手段と、前記正当性判別手段による判別結果を、前記データ保証依頼受信手段によって受信したデータの送信元に送信する判別結果送信手段とを具備したことを特徴とする。

【００１２】また本発明は、端末において作成されたデータの作成日時を保証するデータ作成日時保証システムであって、端末より日時データの要求を受信する要求受信手段と、日時データを作成する日時データ作成手段と、前記要求受信手段により受信した要求に応じて、前記日時データ作成手段によって作成された日時データを前記要求受信手段によって受信した要求の送信元に送信する日時データ送信手段とを具備したことを特徴とする。

【００１３】また、公開鍵暗号方式による公開鍵データと共に、この公開鍵データに関する正当性の保証依頼を受信する公開鍵データ保証依頼受信手段と、前記公開鍵データ保証依頼受信手段によって受信した公開鍵データが、端末において作成されたデータを暗号化する際に用いられる書き換え不能な記録媒体に記録された公開鍵暗号方式による秘密鍵データに対応する正当なものであるかを判別する正当性判別手段と、前記正当性判別手段による判別結果を、前記公開鍵データ保証依頼受信手段によって受信した公開鍵データの送信元に送信する判別結果送信手段とを具備したことを特徴とする。

【００１４】

【発明の実施の形態】以下、図面を参照して本発明の実施の形態について説明する。図１は、第１乃至第３実施形態におけるシステムの構成を示すブロック図である。図１に示すように、センターシステム１０（データ作成日時保証システム）は、インターネット、公衆回線網などの各種通信系を含むネットワーク１１を介して、一般ユーザが使用する端末１２，１４、端末１２，１４を使用するユーザが口座を開設している銀行の銀行サーバ１６等と接続される。

【００１５】センターシステム１０は、データ作成日時保証サービスを提供するもので、端末１２，１４において作成されたデータに対して、自システム内で発生させた日時データをもとにデータ作成日時が保証されるよう

にする。センターシステム１０は、端末１２，１４に対してデータ作成日時保証サービスの提供することで課金を行ない、端末１２，１４のユーザが口座を開設している銀行の銀行サーバ１６より課金料金を徴収する。

【００１６】端末１２，１４は、一般のユーザによって使用されるもので、ユーザからの指示に応じてアプリケーションプログラムにより各種処理を実行する。図１では、端末１２において、アプリケーションプログラムによりデータを作成し、このデータに対するデータ作成日時の証明をセンターシステム１０に依頼するものとし、端末１４において、端末１２で作成されたデータについて、その作成日時を確認するものとして説明する。

【００１７】銀行サーバ１６は、端末１２，１４のユーザが開設している銀行口座を持つ銀行のサーバであり、ネットワーク１１を通じて受信した指示に応じて銀行口座に対する操作を行うことができる。

【００１８】図１中に示すセンターシステム１０、端末１２，１４、銀行サーバ１６は、各種の記録媒体に記録されたプログラムを読み込み、この読み込んだプログラムによって動作が制御されるコンピュータによって構成される。例えば、端末１２，１４は、パーソナルコンピュータ、ＰＤＡ（personal digital assistant）、携帯電話などの個人ユーザにより使用されるように構成されたもので、センターシステム１０は、サーバシステム等の比較的大規模に構成されたものである。

【００１９】図１にはセンターシステム１０の主要な構成部分のみを示している。図１に示すように、センターシステム１０は、ＣＰＵ２０が記憶部２１、通信部２２、及び時計部２３と相互に接続されている。

【００２０】ＣＰＵ２０は、センターシステム１０全体の制御を司るもので、記憶部２１に記録されたプログラムを実行することにより各種の処理を実行する。ＣＰＵ２０は、記憶部２１に記録された日時保証サービスプログラム２１ａを実行することにより、端末１２が作成したデータについて作成日時を保証するためのデータ作成日時保証サービスを実現する。

【００２１】記憶部２１は、ＣＰＵ２０によってアクセスされるプログラムやデータの情報が記録されるもので、本実施形態では例えば日時保証サービスプログラム２１ａなどの各種プログラムや、各プログラムを実行する際に用いられる各種データの他、作業用のデータを一時的に記録するためのワークエリアなどが設定される。日時保証サービスプログラム２１ａの実行に伴って格納される各種データとしては、公開鍵暗号方式による暗号化に用いる暗号鍵データ２１ｂ（秘密鍵データ）、暗号鍵データ２１ｂを用いた暗号化の処理対象となる処理データ２１ｃ（第１及び第２実施形態では文書データ（文書ダイジェスト）、第３実施形態では日時データ）、データ作成日時保証サービスを提供したことに対するユーザへの課金に関する課金データ２１ｄなどが含まれている。

【００２２】記憶部２１は、記憶媒体を有しており、記憶媒体に対するプログラム、データ等の記録や読み出しを実行する。記憶媒体は磁気的、光学的記録媒体、もしくは半導体メモリで構成され、記憶部２１に固定的に設けたもの、もしくは着脱自在に装着するものである。また、記憶媒体に記録されるプログラム、データ等は、通信回線等を介して接続された他の機器から受信して記録する構成にしても良く、さらに、通信回線等を介して接続された他の機器側に記録媒体を備えた記録装置を設け、この記録媒体に記録されているプログラムやデータを、通信回線を介して使用する構成にしても良い。記憶部２１は、記憶媒体に対して各種アプリケーションによって使用される各種のデータ等も記録し、必要に応じて読み出して利用することができる。

【００２３】通信部２２は、ＣＰＵ２０の制御のもとでネットワーク１１を介した他の電子機器（端末１２，１４、銀行サーバ１６など）との通信を制御する。時計部２３は、年月日時刻を表す日時データを発生してＣＰＵ２０に提供する。時計部２３は、例えばセンターシステム１０の動作と関係なく正確な日時データを発生することができるように特別なハードウェアによって構成されているものとする。

【００２４】また、図１には端末１２の主要な構成部分のみを示している。図１に示すように、端末１２は、ＣＰＵ３０が記憶部３１、通信部３２、入力部３３、及び表示部３４と相互に接続されている。

【００２５】ＣＰＵ３０は、端末１２全体の制御を司るもので、記憶部３１に記録されたプログラムを実行することにより各種の処理を実行する。ＣＰＵ３０は、記憶部３１に記録されたアプリケーションプログラム３１ｂを実行することにより、このアプリケーションに用いられるデータを作成する。以下の説明では、アプリケーションプログラム３１ｂが文書作成用プログラムであり、文書データを作成するものとして説明する。また、ＣＰＵ３０は、日時保証サービスプログラム３１ａを実行することにより、例えばアプリケーションプログラム３１ｂによって作成されたデータについての作成日時の保証要求がユーザから指示された場合に、センターシステム１０が提供するデータ作成日時保証サービスを利用してデータ作成日時が保証されるようにする処理を実行する。

【００２６】記憶部３１は、ＣＰＵ３０によってアクセスされるプログラムやデータの情報が記録されるもので、本実施形態では例えば日時保証サービスプログラム３１ａ、アプリケーションプログラム３１ｂなどの各種プログラムや、各プログラムを実行する際に用いられる各種データの他、作業用のデータを一時的に記録するためのワークエリアなどが設定される。

【００２７】記憶部３１は、記憶媒体を有しており、記

憶媒体に対するプログラム、データ等の記録や読み出しを実行する。記憶媒体は磁気的、光学的記録媒体、もしくは半導体メモリで構成され、記憶部３１に固定的に設けたもの、もしくは着脱自在に装着するものである。また、記憶媒体に記録されるプログラム、データ等は、通信回線等を介して接続された他の機器から受信して記録する構成にしても良く、さらに、通信回線等を介して接続された他の機器側に記録媒体を備えた記録装置を設け、この記録媒体に記録されているプログラムやデータを、通信回線を介して使用する構成にしても良い。記憶部３１は、記憶媒体に対して各種アプリケーションによって使用される各種のデータ等も記録し、必要に応じて読み出して利用することができる。

【００２８】通信部３２は、ＣＰＵ３０の制御のもとでネットワーク１１を介した他の電子機器（センターシステム１０、端末１４など）との通信を制御する。入力部３３は、キーボードや、マウスなどポインティングデバイスにより構成され、データや各種の指示を入力するために用いられる。表示部３４は、各種情報を表示するためのもので、記憶部３１に格納された各種プログラムの実行に伴う画面を表示する。なお、図１に示す端末１４は、端末１２と同様に記憶部、通信部、入力部、及び表示部などの構成を有しているものとする。端末１４の記憶部には必要に応じて各種プログラムが記憶され、このプログラムが実行されるで各種処理を実行することができる。

【００２９】次に、本発明の第１実施形態の動作について説明する。図２は第１実施形態におけるセンターシステム１０が提供するデータ作成日時保証サービスの概略を説明するための図、図３はセンターシステム１０と端末１２における動作を説明するためのフローチャート、図４はセンターシステム１０と端末１４における動作を説明するためのフローチャートである。

【００３０】まず、端末１２は、アプリケーションプログラム３１ｂによって、ユーザからの指示に応じて文書データを作成したものとする（ステップＡ１）。端末１２を使用するユーザは、作成した文書について作成日時の証明が欲しい場合には、所定の操作により入力部３３から作成日時の証明要求を入力する（ステップＡ２）。

【００３１】ＣＰＵ３０は、所定の操作によって作成日時の証明要求が入力されると、日時保証サービスプログラム３１ａを起動し、このプログラムに従う処理を実行する。まず、ＣＰＵ３０は、作成日時の証明対象とする文書データ（以下、元文書データと称する）について文書ダイジェストを作成する（ステップＡ３）。文書ダイジェストは、例えば予め決められた固定長の数学的抄録データであり、元文書データに対してハッシュ関数を用いて生成するものとする。なお、文書ダイジェストの作成の対象となるデータは、文書データだけでなく、文書データのファイル作成時にファイルと対応づけて記憶されるタイムスタンプのデータが含まれていても良い。

【００３２】ＣＰＵ３０は、文書ダイジェストを作成すると、通信部３２からネットワーク１１を通じて、センターシステム１０に対してデータ作成日時保証サービスの提供依頼と共に文書ダイジェストを送信する（ステップＡ４、図２（１））。

【００３３】一方、センターシステム１０のＣＰＵ２０は、日時保証サービスプログラム２１ａに基づいて、通信部２２によって端末１２からデータ作成日時保証サービスの提供依頼と共に文書ダイジェストを受信すると、処理データ２１ｃとして一時的に記憶部２１に格納すると共に（ステップＢ１）、時計部２３によって発生される現在の年月日時刻を表す日時データを取得する（ステップＢ２）。

【００３４】そして、ＣＰＵ２０は、時計部２３から取得した日時データと、端末１２から取得した文書ダイジェストとを不可分な形で統合し、この統合したデータを予めセンターシステム１０において用意されている暗号鍵データ２１ｂに含まれる公開鍵暗号方式による秘密鍵データを用いて、所定の暗号化アルゴリズムに従って暗号化して署名データを生成する（ステップＢ３）。センターシステム１０において用意されている暗号鍵データ２１ｂ（秘密鍵データ）は、センター側でユーザによって取得されないよう管理されている。

【００３５】センターシステム１０は、秘密鍵データをもとに暗号化して得られた署名データと、この暗号化に用いた秘密鍵データに対応する公開鍵暗号方式による公開鍵データとを端末１２に送信する（ステップＢ４、図２（２））。

【００３６】また、センターシステム１０は、端末１２のユーザへの課金に関する課金データ２１ｄを設定して記憶する。センターシステム１０は、例えば予め設定された期間毎（月末毎など）に、各ユーザについて設定されている課金データ２１ｄに基づいて端末１２のユーザが開設している口座を持つ銀行の銀行サーバ１６にアクセスして、所定の課金金額を徴収する。なお、センターシステム１０は、サービス料を課金する場合には、データ作成日時保証サービスを利用するユーザに対して、予めユーザに関する情報（氏名、課金口座、連絡先など）を登録しておくものとする。そして、ユーザに関する情報の登録時に各ユーザに対してデータ作成日時保証サービスを利用する際のパスワードなどを発行しておき、このパスワードを利用時に指定させることで、課金対象とするユーザ（課金口座）を識別するものとする。

【００３７】一方、端末１２は、センターシステム１０から署名データと公開鍵データとを受信すると、作成した文書データと対応づけて記憶しておく。そして、文書データを外部に公開する場合（図２（３））、例えば端末１４のユーザにネットワーク１１を通じて提供する場合には、文書データに署名データと公開鍵データとを添

付して送信する（ステップＡ５）。

【００３８】なお、前述した説明では、端末１２からセンターシステム１０に対してハッシュ関数等を用いて作成された文書ダイジェストを送信するものとしているが、端末１２において作成された文書データの全てをセンターシステム１０に送信して、センターシステム１０において文書データを文書ダイジェスト化するようにしても良い。

【００３９】また、端末１２において文書データ作成時に、センターシステム１０が提供するデータ作成日時保証サービスを利用して作成日時の保証を得るものとしているが、文書データを作成した後、例えばユーザからの指示に応じて実行するようにしても良い。基本的には、データ作成時と同時に作成日時の保証を受ける方が望ましいが、任意のタイミングで作成日時の保証を受けたとしても、少なくともその日時保証を受けた日時以前に文書が作成されたことを保証することができる。

【００４０】こうして、端末１２において作成された文書データについて、センターシステム１０が提供するデータ作成日時保証サービスを利用して、文書データの作成日時を保証するための署名データを文書データに添付して公開することができる。

【００４１】次に、端末１４において、端末１２により公開された文書データの作成日時を確認しようとする場合について、図４に示すフローチャートを参照しながら説明する。なお、証明付き公開文書を読むことができるプログラムが一般に公開されており、センターシステム１０によるデータ作成日時保証サービスを利用して署名データが添付された文書データについてもこのプログラムによって読むことができるものとする。端末１４には、このプログラムが記憶されており、このプログラムを実行することで以下のようにして端末１２により公開された署名データが添付された文書データを読むことができる。

【００４２】まず、端末１４は、端末１２により公開された文書データと共に、署名データと公開鍵データとを受信し（ステップａ１）、この受信した文書データについての確認指示がユーザにより入力されると、文書データに添付されていた公開鍵データを用いて署名データを解読することによって文書ダイジェストと日時データとを取得する。

【００４３】端末１４は、文書データに対してハッシュ関数により文書ダイジェストを生成し、この生成した文書ダイジェストと署名データを解読することにより得られた文書ダイジェストとを比較することで、文書データの内容が改ざんされているか否かを確認する。すなわち、両者が同一であれば文書データの内容が改ざんされていないと判別することができる。さらに、端末１４は、文書データの内容が改ざんされているか否かの判別結果に応じて、日時データが改ざんされているか否かを確認する（ステップａ２、図２（４））。すなわち、署名データは、センターシステム１０において、文書ダイジェストと日時データとを統合して暗号化されたデータであるため、署名データを復号化して得た文書データが改ざんされていなければ、日時データについても改ざんされていないことが保証される。従って、端末１４のユーザは、保証された日時データによって端末１２により公開された文書の作成日時を確認することができる。

【００４４】さらに第１実施形態においては、センターシステム１０は、端末１２により公開された署名データを復号化する際に用いた公開鍵データについての正当性を保証するためのサービスを提供する。これは、センターシステム１０における暗号化で用いられる暗号化アルゴリズムが盗まれた場合、改ざんされた文書データあるいは日時データに対して、この暗号化アルゴリズムにより不正な秘密鍵データを用いて暗号化され、この暗号化で用いられた秘密鍵データに対応する公開鍵データが署名データに添付されて公開されてしまうおそれがあるためである。この場合、前述したように署名データに対して、この署名データに添付された公開鍵データによって復号化すると、文書ダイジェストと日時データとが共に正当であると判定されてしまう。

【００４５】端末１４は、端末１２が公開した署名データに対する公開鍵データの保証依頼と共に、公開鍵データをセンターシステム１０に対してネットワーク１１を通じて送信する（ステップａ３、図２（５））。

【００４６】センターシステム１０は、端末１４から公開鍵データの保証依頼と共に、保証対象とする公開鍵データを受信すると（ステップＢ６）、この公開鍵データについての正当性を判別するための正当性判別処理を実行する（ステップＢ７）。正当性判別処理では、保証対象とする公開鍵データが署名データを生成（暗号化）する際に用いた秘密鍵データに対応するものか、すなわちセンターシステム１０が管理する秘密鍵データを用いて暗号化したデータを保証対象とする公開鍵データによって復号化した時に正しいデータが得られるか否かによって判別する。

【００４７】センターシステム１０は、正当性判別処理によって得られた結果を正当性に関する回答として、公開鍵データの保証依頼元である端末１４に対して送信する（ステップＢ８、図２（６））。

【００４８】端末１４は、センターシステム１０から正当性回答を受信し、公開鍵データが正当であるか否かを確認することができる（ステップａ４）。

【００４９】このようにして、第１実施形態のセンターシステム１０は、端末１２において作成された文書データ（文書ダイジェスト）に対して、センターシステム１０において生成した信頼性の高い日時データを不可分な形で統合して、ユーザにより取得できない秘密鍵データを用いて暗号化するため、文書データと日時データの両

方について、第３者だけでなく文書の作成者によっても改ざんすることができないため、文書の作成が日時データにより示される日時（少なくともそれ以前）に行われたことを文書作成後であっても保証することができる。また、公開鍵暗号方式による公開鍵データを用いて日時データの検証をすることができるので、何時でも誰によっても文書の作成日時を確認することができる。

【００５０】なお、前述した説明では、データ作成日時保証サービスによる保証の対象が文書データと日時データであるとしているが、文書の作成者を表す作成者データを保証対象に含めるようにしても良い。この場合、センターシステム１０では、文書ダイジェストと日時データと作成者データとを統合して暗号化し、この暗号化により得られた作成者データを含む署名データを端末１２に送信する。以下、作成者データについても日付データと同様に処理することで、文書データの作成日時と共に文書の作成者についても保証することができる。

【００５１】また、端末１２からは文書全体を公開するものとしているが、作成文書の抄録などを作成日時の保証を付けて公開することで、文書全体を秘匿した状態で、文書が作成されたことについて証明することもできる。

【００５２】次に、本発明の第２実施形態の動作について説明する。図５は第２実施形態におけるセンターシステム１０が提供するデータ作成日時保証サービスの概略を説明するための図、図６はセンターシステム１０において管理される署名データベース１０ａ（後述する）に登録されるデータの一例を示す図、図７（ａ）（ｂ）はセンターシステム１０と端末１２における動作を説明するためのフローチャート、図８（ａ）（ｂ）はセンターシステム１０と端末１４における動作を説明するためのフローチャートである。

【００５３】なお、図７（ａ）のフローチャートに示すステップＣ１～Ｃ４の処理については、前述した図３（ａ）のフローチャートに示すステップＡ１～Ａ４の処理と同様にして実行されるものとして詳細な説明を省略する。

【００５４】端末１２により文書が作成され、日時証明の操作がなされると、ＣＰＵ３０は、文書ダイジェストを作成し、通信部３２からネットワーク１１を通じて、センターシステム１０に対してデータ作成日時保証サービスの提供依頼と共に文書ダイジェストを送信する（ステップＣ４、図５（１））。

【００５５】一方、センターシステム１０のＣＰＵ２０は、日時保証サービスプログラム２１ａに基づいて、通信部２２によって端末１２からデータ作成日時保証サービスの提供依頼と共に文書ダイジェストを受信すると、処理データ２１ｃとして一時的に記憶部２１に格納すると共に（ステップＤ１）、時計部２３によって発生される現在の年月日時刻を表す日時データを取得する（ステップＤ２）。

【００５６】そして、ＣＰＵ２０は、時計部２３から取得した日時データと、端末１２から取得した文書ダイジェストとを不可分な形で統合し、この統合したデータを予めセンターシステム１０において用意されている暗号鍵データ２１ｂに含まれる公開鍵暗号方式による秘密鍵データを用いて、所定の暗号化アルゴリズムに従って暗号化して署名データを生成する（ステップＤ３）。センターシステム１０において用意されている暗号鍵データ２１ｂ（秘密鍵データ）は、センター側でユーザによって取得されないよう管理されている。

【００５７】センターシステム１０は、秘密鍵データをもとに暗号化して得られた署名データと、この暗号化に用いた秘密鍵データ（暗号化鍵データ）とを対応づけて署名データベース１０ａとして記憶部２１に登録すると共に、これらの情報を特定するためのリンク情報も対応付けて登録する。そして、センターシステム１０は、署名データベース１０ａに登録したリンク情報のみを端末１２に送信する（ステップＤ４、図５（２））。

【００５８】また、センターシステム１０は、端末１２のユーザへの課金に関する課金データ２１ｄを設定して記憶する（ステップＤ５）。なお、課金に関しては第１実施形態と同様にして行われるものとして詳細な説明を省略する。

【００５９】一方、端末１２は、センターシステム１０からリンク情報を受信すると、作成した文書データと対応づけて記憶しておく。そして、文書データを外部に公開する場合、例えば端末１４のユーザにネットワーク１１を通じて提供する場合には、文書データにリンク情報を添付して送信する（ステップＣ５）。

【００６０】こうして、端末１２において作成された文書データについて、センターシステム１０が提供するデータ作成日時保証サービスを利用して、文書データの作成日時を保証するための署名データをセンターシステム１０の署名データベース１０ａに登録しておくことができる。従って、センターシステム１０に作成文書の保証依頼をした後では、端末１２のユーザであっても文書内容、作成日付を変更することができない。また、センターシステム１０から端末１２に対してはリンク情報のみを返信するので通信に要するコストを低減することができる。

【００６１】次に、端末１４において、端末１２により公開された文書データの作成日時を確認しようとする場合について、図８（ａ）（ｂ）に示すフローチャートを参照しながら説明する。なお、第２実施形態においても、端末１４には証明付き公開文書を読むことができるプログラムが記憶されており、このプログラムを実行することで以下のようにして端末１２により公開された文書データを読むことができると共にセンターシステム１０において管理されている文書の作成日を示す日付データ

の確認ができるものとする。

【００６２】まず、端末１４は、端末１２により公開された文書データと共にリンク情報を受信し（ステップｃ１）、この受信した文書データについての確認指示がユーザにより入力されると、文書データに対してハッシュ関数により文書ダイジェストを生成し、端末１２が公開した文書の保証依頼と共に生成した文書ダイジェストとリンク情報とをセンターシステム１０に対してネットワーク１１を通じて送信する（ステップｃ２、図５（４））。

【００６３】第２実施形態においては、センターシステム１０は、端末１２により公開された文書に添付されたリンク情報をもとに、署名データベース１０ａにおいて管理している署名データを特定し、この特定された署名データをもとに文書の正当性を保証すると共に文書の作成日時を確認するためのサービスを提供する。

【００６４】センターシステム１０は、端末１４から文書の保証依頼と共に、保証対象とする文書の文書ダイジェストとリンク情報を受信すると（ステップＤ６）、文書と日付データについての正当性を判別するための正当性判別処理を実行する（ステップＤ７）。正当性判別処理では、端末１４から受信したリンク情報をもとに、署名データベース１０ａに登録されたリンク情報が示す署名データを特定する。そして、特定した署名データと対応づけて登録された秘密鍵データ（暗号化鍵データ）に対応する公開鍵データを用いて署名データを復号化（解読）し、文書ダイジェストと日付データとを生成する。センターシステム１０は、復号化によって生成した文書ダイジェストと端末１４から受信した文書ダイジェストとを比較することによって、端末１２により公開された文書（端末１４からの文書ダイジェスト）が正当であるかを判別する。すなわち、文書ダイジェストが一致する場合には、端末１２により生成されてセンターシステム１０により作成日時保証を受けた文書が改ざんされることなく公開されたものと判別できる。また、文書ダイジェストが一致することで、復号化により生成された日付データも正当であり、この日付データが示す日時（少なくともそれ以前）に文書が作成されたことを確認することができる。

【００６５】センターシステム１０は、正当性判別処理によって得られた結果を正当性に関する回答として、公開鍵データの保証依頼元である端末１４に対して送信する（ステップＤ８、図５（６））。文書内容が正当（改ざんされていない）と判別された場合には、センターシステム１０は、日時データも端末１４に対して送信する。

【００６６】端末１４は、センターシステム１０から正当性回答を受信し、文書内容が正当であるか否かを確認し、正当である場合には文書作成日時を示す日時データを受信することができる（ステップｃ３）。

【００６７】このようにして、第２実施形態のセンターシステム１０は、端末１２において作成された文書データ（文書ダイジェスト）に対して、センターシステム１０において生成した信頼性の高い日時データを不可分な形で統合して、ユーザにより取得できない秘密鍵データを用いて暗号化し、署名データベース１０ａにおいて登録して管理するので、文書データと日時データの両方について、第３者だけでなく文書の作成者によっても改ざんすることができず、文書の作成が日時データにより示される日時（少なくともそれ以前）に行われたことを文書作成後であっても保証することができる。また、端末１２，１４では、センターシステム１０によるデータ作成日時保証サービスを利用することにより得た文書に対するリンク情報のみを保持していれば、任意に作成文書の内容の正当性と作成日時の確認を行うことができるので管理を容易にすることができる。

【００６８】なお、前述した説明では、データ作成日時保証サービスによる保証の対象が文書データと日時データであるとしているが、第１実施形態と同様にして、文書の作成者を表す作成者データを保証対象に含めるようにしても良い。

【００６９】次に、本発明の第３実施形態の動作について説明する。図９は第３実施形態におけるセンターシステム１０が提供するデータ作成日時保証サービスの概略を説明するための図、図１０は（ａ）（ｂ）はセンターシステム１０と端末１２における動作を説明するためのフローチャートである。

【００７０】第３実施形態では、センターシステム１０が提供するデータ作成日時保証サービスを利用して、端末１２において作成した文書についての作成日時保証を受けるためには、センターシステム１０の例えば管理者が配布するＩＣカード４０が用いられる。ＩＣカード４０は、所定の暗号化プログラム４１と、この暗号化プログラム４１による暗号化で使用される公開鍵暗号方式による秘密鍵データ４２とが記録された記録内容を書き換え不能な記録媒体であり、端末１２に装着されることで使用される。

【００７１】まず、端末１２は、アプリケーションプログラム３１ｂによって、ユーザからの指示に応じて文書データを作成したものとする（ステップＥ１）。端末１２を使用するユーザは、作成した文書について作成日時の証明が欲しい場合には、所定の操作により入力部３３から作成日時の証明要求を入力する（ステップＥ２）。

【００７２】ＣＰＵ３０は、所定の操作によって作成日時の証明要求が入力されると、日時保証サービスプログラム３１ａを起動し、このプログラムに従う処理を実行する。まず、ＣＰＵ３０は、作成日時の証明対象とする元文書データについて第１実施形態と同様にして文書ダイジェストを作成する（ステップＥ３）。

【００７３】ＣＰＵ３０は、文書ダイジェストを作成す

ると、通信部３２からネットワーク１１を通じて、センターシステム１０に対して日時データの送信を要求する（ステップＥ４、図９（１））。

【００７４】一方、センターシステム１０のＣＰＵ２０は、日時保証サービスプログラム２１ａに基づいて、通信部２２によって端末１２から日時データの送信要求を受信すると（ステップＦ１）、時計部２３によって発生される現在の年月日時刻を表す日時データを取得する（ステップＦ２）。

【００７５】そして、ＣＰＵ２０は、時計部２３から取得した日時データに対して、予めセンターシステム１０において用意されている暗号鍵データ２１ｂに含まれる公開鍵暗号方式による秘密鍵データを用いて、所定の暗号化アルゴリズムに従って暗号化する（ステップＦ３）。センターシステム１０において用意されている日時データに対する暗号鍵データ２１ｂ（秘密鍵データ）は、センター側でユーザによって取得されないよう管理されている。

【００７６】センターシステム１０は、秘密鍵データをもとに暗号化した日時データを端末１２に送信する（ステップＦ４、図９（２））。

【００７７】また、センターシステム１０は、端末１２のユーザへの課金に関する課金データ２１ｄを設定して記憶する。なお、課金に関しては第１実施形態と同様にして行われるものとして詳細な説明を省略する。

【００７８】一方、端末１２は、センターシステム１０から暗号化された日時データを受信すると（ステップＥ５）、この暗号化に用いた秘密鍵データに対応する公開鍵暗号方式による公開鍵データを用いて日時データを復号化する。

【００７９】そして、端末１２は、センターシステム１０から取得した日時データと、先に作成した文書ダイジェストとを不可分な形で統合し、この統合したデータをＩＣカード４０に記憶された公開鍵暗号方式による秘密鍵データ４２を用いて、暗号化プログラム４１に従って暗号化して署名データを生成する（ステップＥ７，図９（３））。

【００８０】文書データを外部に公開する場合、例えば端末１４のユーザにネットワーク１１を通じて提供する場合には、文書データにＩＣカード４０を用いて生成した署名データと、ＩＣカード４０に格納された秘密鍵データ４２に対応する公開鍵データとを添付して送信する（ステップＥ８、図９（４））。

【００８１】なお、前述した説明では、ＩＣカード４０に格納された暗号化プログラム４１により署名データを生成する処理のみを実行するように説明しているが、端末１２のユーザから作成日時の証明要求が入力された以降の処理をユーザからの指示によらず暗号化プログラム４１に従って実行するようにしても良い。

【００８２】こうして、センターシステム１０から取得した日時データと文書ダイジェストとを統合し、ＩＣカード４０を用いて署名データを生成し、端末１２において作成された文書データに対して添付して公開することができる。第３実施形態では、ＩＣカード４０がなければセンターシステム１０から取得した日時データと文書データとを統合した暗号化をすることができないため、ＩＣカード４０を有していない第３者が文書データや日時データを改ざんして署名データを生成することができないので、文書データと日時データとの正当性を保証することができる。

【００８３】一方、端末１４においては、端末１２により公開された文書データの作成日時を確認しようとする場合には、ＩＣカード４０の暗号化プログラム４１と秘密鍵データ４２に対応する公開鍵データを用いて署名データを復号化することで、文書の作成日付を確認することができる（図９（５））。なお、第３実施形態における端末１４で実行される処理（公開鍵の正当性の確認など（図９（５）（６））については、第１実施形態と同様にして実行されるものとして詳細な説明を省略する。

【００８４】なお、前述した説明では、端末１２において署名データを生成するために用いる暗号化プログラム４１と秘密鍵データ４２とをＩＣカード４０によって提供するものとしているが、暗号化プログラム４１と秘密鍵データ４２とをハードウェア（ファーム）化して端末１２に組み込むようにしても良い。暗号化プログラム４１と秘密鍵データ４２とをハードウェア化することで、ユーザによる処理過程でのデータの改ざんを防止することができる。

【００８５】また、前述した説明では、センターシステム１０から提供される日時データが端末１２からの要求に応じてネットワーク１１を通じて送信されるものとしているが、放送局から日時データ放送（または極狭帯域通信）などの方式によって一方的に日時データを送出する形態としても良い。この場合、端末１２は、日時データ放送を受信する機能が搭載され、この機能により受信した電波から日時データを分離して署名データの生成に利用する。

【００８６】次に、第３実施形態に対する改良の一例について説明する。前述した第３実施形態では、ＩＣカード４０を用いて端末１２において文書データと日時データに対する暗号化（署名データの生成）をしているため、ＩＣカード４０が第３者に渡らなければ文書データや日時データに対する改ざんのおそれはないが、ＩＣカード４０や暗号化アルゴリズム、秘密鍵データ自体が悪意のある第３者によって盗まれた場合には、その第３者による不正を回避することができなくなってしまう。

【００８７】そこで、センターシステム１０は、さらに日時データが第３者による改ざんされていないことを保証するための日時問い合わせ応答サービスを提供する。

21

【００８８】このために、センターシステム１０は、再現性のない事象をもとにした付加データを作成する機能と、この機能により作成された付加データを端末１４に提供する日時データと対応づけて付加日時データベース１０ｂに登録しておく機能が設けられる。図１１には付加日時データベース１０ｂに格納されるデータの一例を示している。

【００８９】センターシステム１０は、端末１２から日時データの送信要求を受信した場合、時計部２３によって発生される現在の年月日時刻を表す日時データを取得すると共に付加データを生成し、この日時データと付加データとを対応づけて付加日時データベース１０ｂに登録しておく。また、日時データと付加データと統合して暗号化し、端末１２に暗号化された日時データとして送信する。

【００９０】再現性のない事象をもとにした付加データとしては、例えば自然現象や生体現象をもとにしたデータや、機器が発生する誤差を含むデータなどを利用することができる。機器が発生する誤差を含むデータとしては、例えばセンターシステム１０内に設置されたデジタル温度センサーの熱雑音を含めた下位１ビットの５０ｍｓごとに２０回測定した２０ビット列のデータ（この場合、１秒に対する付加データ）がある。

【００９１】以下、第３実施形態と同様にして、端末１２では付加データを含めて署名データを生成して端末１４に送信する。

【００９２】一方、端末１４は、端末１２から公開された文書の作成日時を確認するために、公開鍵データの正当性の保証依頼と同様にして、日時データの正当性の保証依頼と共に日時データと付加データとをセンターシステム１０に送信する（図９（５））。

【００９３】。

【００９４】センターシステム１０は、端末１４から日時データと付加データと共に、これらのデータに関する正当性の保証依頼を受信すると、受信した日時データと付加データとが正当なものであるかを、付加日時データベース１０ｂに格納された日時データと付加データとをもとに判別する。すなわち、センターシステム１０は、端末１４からの日時データと付加データとの対応関係が付加日時データベース１０ｂに登録されている場合には、日時データが改ざんされていないものと判別することができる。センターシステム１０は、この判別結果を回答として、日時データの保証依頼元である端末１４に対して送信する（図９（６））。

【００９５】このようにして、日時データに付加された付加データは、センターシステム１０の付加日時データベース１０ｂにおいて管理されているため、端末１２において作成された文書の作成日付が万が一改ざんされたとしても、付加日時データベース１０ｂに登録されている日時データと付加データとが一致しなくなるため、改ざんされたことを容易に判別することができる。これにより、日時データに対するセキュリティレベルをより向上させることができる。なお、前述した日時問い合わせ応答サービスは、第３実施形態に限らず第１実施形態、第２実施形態のそれぞれに対して適用することができる。

22

【００９６】また、前述した各実施形態においては、文書作成が行われる端末１２のユーザに対して課金を行うものとして説明しているが、データ作成日時保証サービスを利用して端末１２において作成された日時を確認する端末１４のユーザに対して課金するようにしても良い。この場合、端末１４のユーザに対しても、予めユーザに関する情報（氏名、課金口座、連絡先など）を登録しておくと共にデータ作成日時保証サービスを利用する際のパスワードなどを発行しておき、このパスワードを利用時に指定させることで、課金対象とするユーザ（課金口座）を識別するものとする。

【００９７】また、本発明は、前述した実施形態に限定されるものではなく、実施段階ではその要旨を逸脱しない範囲で種々に変形することが可能である。また、前述した実施形態で実行される機能は可能な限り適宜組み合わせて実施しても良い。前述した実施形態には種々の段階の発明が含まれており、開示される複数の構成要件における適宜の組み合わせにより種々の発明が抽出され得る。例えば、実施形態に示される全構成要件から幾つかの構成要件が削除されても、効果が得られるので有れば、この構成要件が削除された構成が発明として抽出され得る。

【００９８】また、前述した各実施形態において記載した処理は、コンピュータに実行させることのできる日時保証プログラムとして、例えば磁気ディスク（フロッピー（登録商標）ディスク、ハードディスク等）、光ディスク（ＣＤ－ＲＯＭ、ＤＶＤ等）、半導体メモリなどの記録媒体に書き込んで各種装置に提供することができる。また、通信媒体により伝送して各種装置に提供することも可能である。データ作成日時保証サービスを提供するサーバ（データ作成日時保証システム）を実現するコンピュータは、記録媒体に記録された日時保証プログラムを読み込み、または通信媒体を介して日時保証プログラムを受信し、このプログラムによって動作が制御されることにより、上述した処理を実行する。

【００９９】

【発明の効果】以上のように本発明によれば、端末において作成されたデータ（文書など）について、作成された時点（あるいは作成時以降）に作成日時を保証するデータ作成日時保証サービスを提供することができる。データ作成日時保証サービスでは、端末で生成される日時データではなくデータ作成日時保証システムにおいて生成される正確かつ改ざん不能な日時データが用いられるために十分な精度及び信頼性を確保することができる。

【図面の簡単な説明】

【図１】第１乃至第３実施形態におけるシステムの構成を示すブロック図。

【図２】第１実施形態におけるセンターシステム１０が提供するデータ作成日時保証サービスの概略を説明するための図。

【図３】センターシステム１０と端末１２における動作を説明するためのフローチャート。

【図４】センターシステム１０と端末１４における動作を説明するためのフローチャート。

【図５】第２実施形態におけるセンターシステム１０が提供するデータ作成日時保証サービスの概略を説明するための図。

【図６】センターシステム１０において管理される署名データベース１０ａ（後述する）に登録されるデータの一例を示す図。

【図７】センターシステム１０と端末１２における動作を説明するためのフローチャート。

【図８】センターシステム１０と端末１４における動作を説明するためのフローチャート。

【図９】第３実施形態におけるセンターシステム１０が提供するデータ作成日時保証サービスの概略を説明するための図。

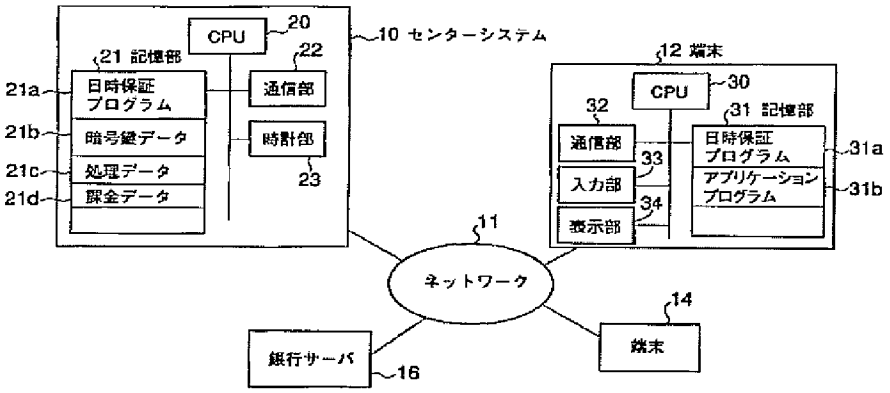
【図１０】センターシステム１０と端末１２における動作を説明するためのフローチャート。

【図１１】付加日時データベース１０ｂに格納されるデータの一例を示す図。

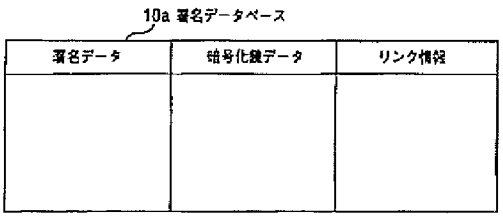
【符号の説明】

１０…センターシステム
１０ａ…署名データベース
１０ｂ…付加日時データベース
１１…ネットワーク
１２，１４…端末
１６…銀行サーバ
２０，３０…ＣＰＵ
２１，３１…記憶部
２１ａ，３１ａ…日時保証プログラム
２１ｂ…暗号鍵データ
２２，３２…通信部
２３…時計部
３３…入力部
３４…表示部
４０…ＩＣカード

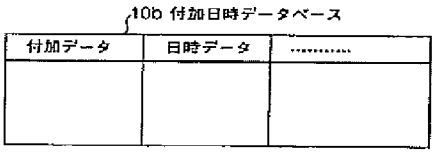
【図１】



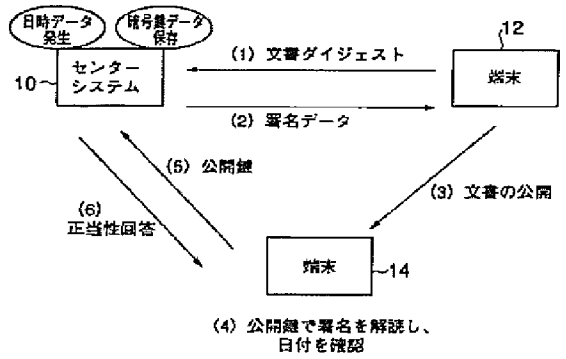
【図６】



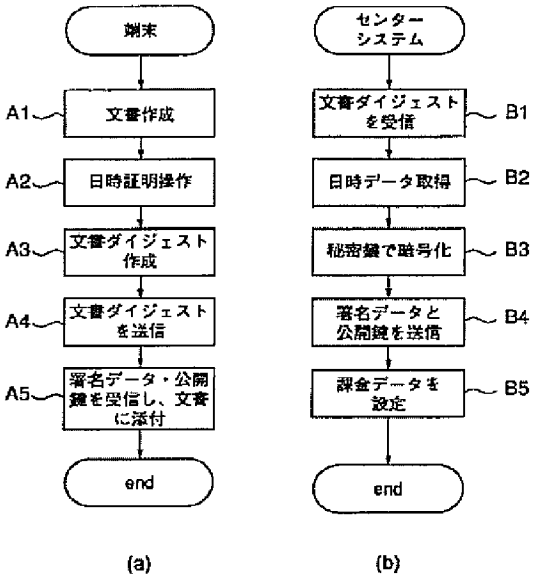
【図１１】



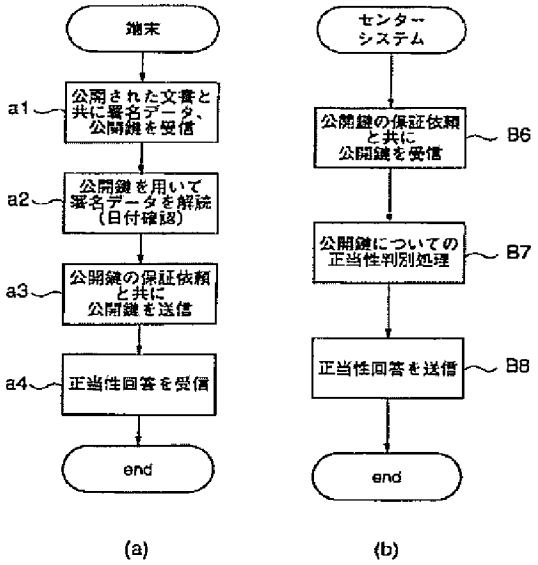
【図２】


日時データ発生
暗号鍵データ保存
センターシステム
10
(1) 文書ダイジェスト
(2) 署名データ
12
端末
(5) 公開鍵
(6) 正当性回答
(3) 文書の公開
端末
14
(4) 公開鍵で署名を解読し、日付を確認

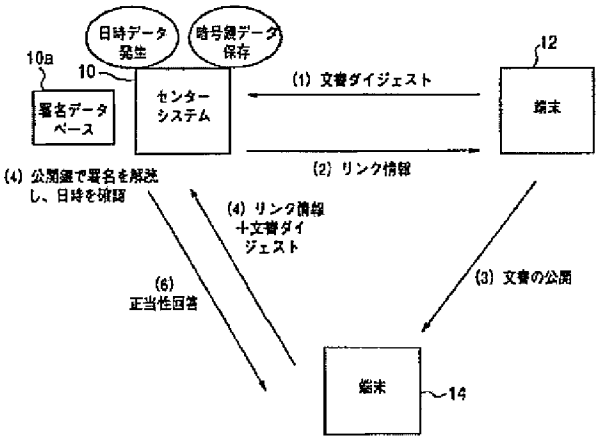
【図３】


端末
A1
文書作成
A2
日時証明操作
A3
文書ダイジェスト作成
A4
文書ダイジェストを送信
A5
署名データ・公開鍵を受信し、文書に添付
end
(a)
センターシステム
文書ダイジェストを受信
B1
日時データ取得
B2
秘密鍵で暗号化
B3
署名データと公開鍵を送信
B4
課金データを設定
B5
end
(b)

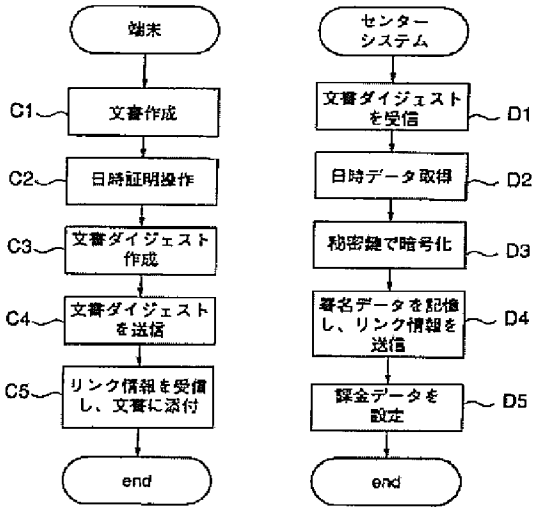
【図４】


端末
a1
公開された文書と共に署名データ、公開鍵を受信
a2
公開鍵を用いて署名データを解読（日付確認）
a3
公開鍵の保証依頼と共に公開鍵を送信
a4
正当性回答を受信
end
(a)
センターシステム
公開鍵の保証依頼と共に公開鍵を受信
B6
公開鍵についての正当性判別処理
B7
正当性回答を送信
B8
end
(b)

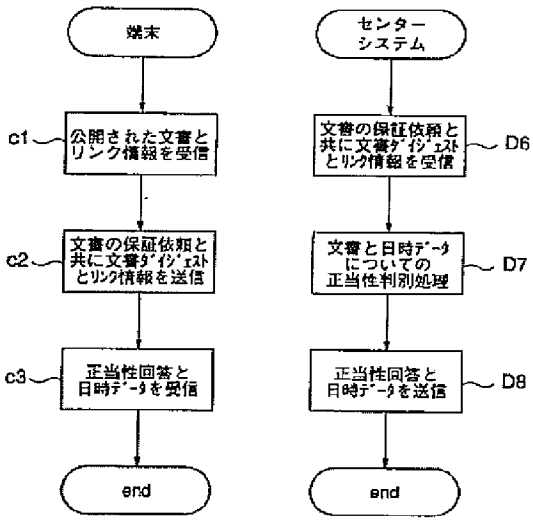
【図５】


日時データ発生
暗号鍵データ保存
10a
署名データベース
10
センターシステム
(1) 文書ダイジェスト
12
端末
(2) リンク情報
(4) 公開鍵で署名を解読し、日時を確認
(4) リンク情報＋文書ダイジェスト
(6) 正当性回答
(3) 文書の公開
端末
14

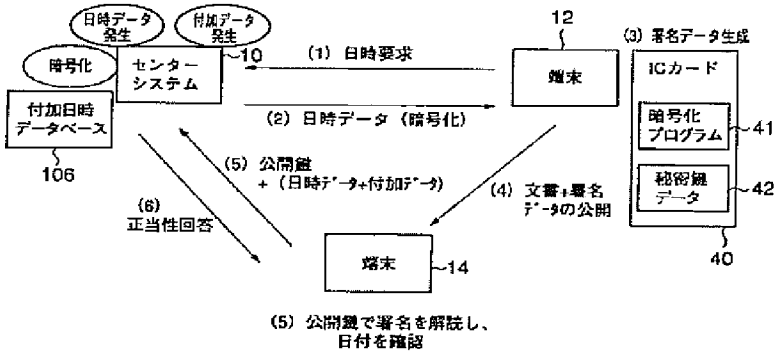
【図７】


端末
C1
文書作成
C2
日時証明操作
C3
文書ダイジェスト作成
C4
文書ダイジェストを送信
C5
リンク情報を受信し、文書に添付
end
センターシステム
文書ダイジェストを受信
D1
日時データ取得
D2
秘密鍵で暗号化
D3
署名データを記憶し、リンク情報を送信
D4
課金データを設定
D5
end
(a)
(b)

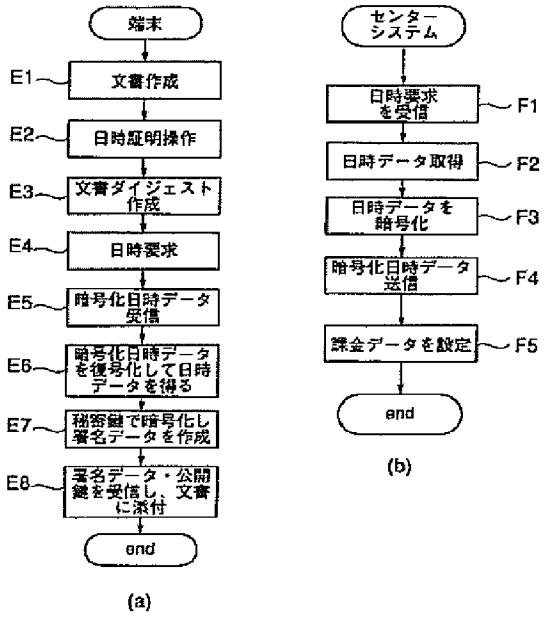
【図８】


端末
c1
公開された文書とリンク情報を受信
c2
文書の保証依頼と共に文書ダイジェストとリンク情報を送信
c3
正当性回答と日時データを受信
end
センターシステム
文書の保証依頼と共に文書ダイジェストとリンク情報を受信
D6
文書と日時データについての正当性判別処理
D7
正当性回答と日時データを送信
D8
end
(a)
(b)

【図９】


日時データ発生
付加データ発生
暗号化
センターシステム
10
付加日時データベース
106
(1) 日時要求
(2) 日時データ（暗号化）
12
端末
(3) 署名データ生成
ICカード
暗号化プログラム
41
秘密鍵データ
42
40
(4) 文書＋署名データの公開
(5) 公開鍵＋（日時データ+付加データ）
(6) 正当性回答
端末
14
(5) 公開鍵で署名を解読し、日付を確認

【図１０】



フロントページの続き

(51) Int. Cl.[7]	識別記号	F I		ﾃｰﾏｺｰﾄﾞ (参考)
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７３Ａ	
			６７５Ｄ	